REMARKS

This submission is in response to the Office Action February 22, 2008.

Applicants have amended the specification in paragraph [0031] to correct an inadvertent error. Applicants have further amended claims 1, 4-9, 13-17, 19 and 20. Support for the amendments herein is found in the specification at least in paragraphs [0023], [0043] and [0048] in view of FIGS 1 - 3. Applicants respectfully submit that no new subject matter has been.

Claims 10-12 have been cancelled without prejudice or disclaimer. No new claims have been added. Consequently, claims 1-9 and 13-20 are pending in this application.

§ 103 Rejection of the Claims

Claims 1-20 were rejected pursuant to 35 U.S.C. § 103(a), as being unpatentable over Deshpande, *et al.* (U.S. Pub. No. 2002/0176579) (hereinafter "Deshpande") in view of Barriga-Caceres, *et al.* (U.S. Pub. No. 2003/0163733) (hereinafter "Barriga).

The primary cited reference to Deshpande is directed to providing location-based services to a wireless device using a hotspot access point. (See Deshpande, Abstract). In FIG. 1, Deshpande discloses a mobile wireless device 40 that connects via hotspot access point 20 and registers with a hotspot service provider network 10, which confirms the user/device's access privileges by confirming authorization with one or more authentication servers 50. (See Deshpande, par. [0020] in view of FIG. 1). Once authorized, the mobile wireless device 40 may request or accept location-based services that are implemented using one or more location-based services servers 60 that are supplied through the hotspot access point 20 and the hotspot service provider network 10. (See Deshpande, par. [0020] in view of FIG 1). In FIG. 2, Deshpande discloses the registration of a mobile wireless device 130 via a hotspot access point 110 with an intranet 100 and confirmation of the user/device's access privileges with one or more authentication servers 140. (See Deshpande, par. [0022] in view of FIG. 2). Once authorized, the device 130 may request or accept e-mail, contacts, task list, calendar and other standard application services via one or more exchange servers 150 and other services such as location-

based services implemented using one or more special application servers 160 and supplied through the hotspot access point 110 and the intranet 100. (See Deshpande, par. [0022] in view of FIG. 2).

The secondary cited reference to Barriga is directed to single sign-on (SSO) services. When a user (*e.g.*, User @MNO-A) wants to use cellular SSO service at a given service provider (SP) (*e.g.*, SP-1), the SP automatically redirects the user's request via the SP's entrance point to the cellular federation, namely an Authentication Broker (AB) (*e.g.*, AB 1), to a site in the federation, namely an Authentication Provider (AP) (*e.g.*, AP 4) of a mobile network operator (MNO-A), that can handle the user's request. (See Barriga, page 5, par. [0066] in view of FIG. 1). The MNO-A creates an authentication assertion for the user specifically addressed for the SP. An artifact referring to the user's authentication assertion is sent to the user and the user presents this artifact to the SP. The SP verifies that the source of the artifact is valid and refers the user's assertion to the user's home site MNO-A. The MNO-A sends back to the SP the complete user's assertion with required user data including authentication information. (See Barriga, page 5, par. [0073] in view of FIG. 2).

In traversing the rejection of independent claim 1, Applicants respectfully submit that the cited portions of Deshpande and Barriga fail to teach or suggest "an authorization engine operable to *issue the user's computing device a token indicating a grant of access rights to both transport services and federated data services of federated data service providers* via the global communications network and the network access hub in response to the authentication of the initial set of credentials, *the token operable to authorize access of the user to both the transport services and the federated data services of the federated data service providers without the user having to provide the initial set of credentials to re-authenticate with the federated service providers*," as particularly recited in claim 1.

On page 3 of the Office Action, the Examiner correctly acknowledged that Deshpande does not teach an authorization engine operable to grant access to both transport services and federated data services of federated service providers. Thus, Applicants respectfully submit that the cited portions of Deshpande further fail to teach or suggest an authorization engine that

issues a token indicating a grant of access rights to both transport services and federated data services of federated data service providers.

The cited portions of Deshpande do not teach or suggest an *authorization engine* that issues the computing device a token indicating access rights to transport services and federated data services of federated service providers. Instead, Deshpande teaches an *authentication server 50* that authenticates a mobile device 40 to its network 10 via hotspot access point 20. In addition, Deshpande's authentication server 50 does not issue its mobile device 40 a token indicating the grant of access rights to both transport services and federated data services of federated data service providers. The cited portions of Deshpande are silent regarding issuing the mobile device 40 a token that is operable to authorize access of the mobile device 40 to both transport services and federated data services of the federated data service providers without the user having to provide the initial set of credentials to re-authenticate with the federated service providers.

The cited portions of Barriga do not rectify the deficiencies identified in Deshpande. The cited portions of Barriga do not teach or suggest an authorization engine that issues the computing device a token indicating access rights to transport services and federated data services of federated service providers. Instead, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider (SP). However, artifact authentication is disparate and distinct from the token-based authorization of claim 1. Barriga's artifact does not indicate access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact method refers to a user's authentication assertion addressed for a single service provider. Thus, the artifact method does not indicate access rights to transport services and access rights to multiple service providers.

In view of the foregoing, Applicants respectfully request the Office to withdraw the rejection pursuant to 35 U.S.C. § 103(a) of independent claim 1. Applicants further respectfully request the Office to withdraw the rejection of dependent claims 2-6, based at least on their dependencies from independent claim 1.

In traversing the rejection of independent claim 7, Applicants respectfully submit that the cited portions of Deshpande and Barriga fail to teach or suggest "issuing to the electronic device via the authorization engine a token indicating a grant of access rights to network transport services and federated network data services of federated data service providers via the global communications network and the network access hub," as particularly recited in claim 7.

The cited portions of Deshpande do not teach or suggest an authorization engine that issues the electronic device a token indicating access rights to transport services and federated data services of federated service providers. Instead, Deshpande teaches an authentication server 50 that authenticates a mobile device 40 to its network 10 via hotspot access point 20. In addition, Deshpande's authentication server 50 does not issue its mobile device 40 a token indicating the grant of access rights to both transport services and federated data services of federated data service providers.

The cited portions of Barriga do not rectify the deficiencies identified in Deshpande. Specifically, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider (SP). However, artifact authentication is disparate and distinct from token-based authorization. Barriga's artifact authentication does not indicate access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact authentication refers to a user's authentication assertion addressed for a *single* service provider. Thus, the artifact authentication does not indicate access rights to transport services and access rights to multiple service providers.

In view of the foregoing, Applicants respectfully request the Office to withdraw the rejection pursuant to 35 U.S.C. § 103(a) of independent claim 7. Applicants further respectfully request the Office to withdraw the rejection of dependent claims 8 and 9, based at least on their dependencies from independent claim 7.

In traversing the rejection of independent claim 13, Applicants respectfully submit that the cited portions of Deshpande and Barriga fail to teach or suggest "an authorization engine communicatively coupled to the broad communications network and operable to issue a token to

an electronic device communicatively coupled to at least a first hotspot of the plurality of hotspots, the token operable as a valid indicator of access rights to both transport services and federated data services of federated data service providers over the broad communications network and the at least one of the plurality of hotspots," as particularly recited in claim 13.

The cited portions of Deshpande do not teach or suggest an authorization engine that issues a token to an electronic device, the token operable as a valid indicator of access rights to transport services and federated data services of federated service providers. Instead, Deshpande teaches an authentication server 50 that authenticates a mobile device 40 to its network 10 via hotspot access point 20. In addition, Deshpande's authentication server 50 does not issue its mobile device 40 a token operable as a valid indicator of access rights to both transport services and federated data services of federated data service providers.

The cited portions of Barriga do not rectify the deficiencies identified in Deshpande. Specifically, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider. However, artifact authentication is disparate and distinct from token-based authorization. Barriga's artifact authentication is not a valid indicator of access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact authentication refers to a user's authentication assertion addressed for a single service provider. Thus, the artifact authentication does not indicate access rights to transport services and access rights to multiple service providers.

In view of the foregoing, Applicants respectfully request the Office to withdraw the rejection pursuant to 35 U.S.C. § 103(a) of independent claim 13. Applicants further respectfully request the Office to withdraw the rejection of dependent claims 14-20, based at least on their dependencies from independent claim 13.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the cited references as applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

5-21-2008
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicant(s)
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)